DTU Library

Mobile network architecture of the long-range WindScanner system

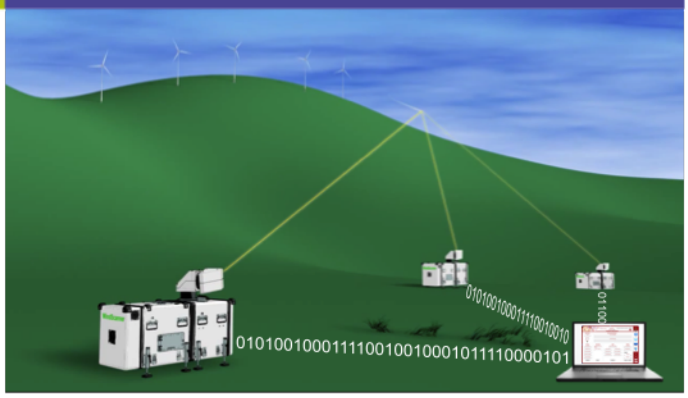
Vasiljevic, Nikola; Lea, Guillaume; Hansen, Per; Jensen, Henrik M.

Publication date:
2016

Document Version
Publisher's PDF, also known as Version of record

Mobile network architecture of the long-range WindScanner system

DTU Wind Energy - Report



Nikola Vasiljević, Guillaume Lea, Per Hansen and Henrik M. Jensen

DTU Wind Energy E-0105

January 2016

DTU Wind Energy
Department of Wind Energy

Authors: Nikola Vasiljević, Guillaume Lea, Per Hansen and Henrik M. Jensen

Title: Mobile network architecture of the long-range WindScanner system

Department: DTU Wind Energy

DTU Wind Energy E-0105

2016

ISBN 978-87-93278-61-5

Sponsorship:
WindScanner.EU

Contact information:
niva@dtu.dk (Nikola Vasiljević)

Pages: 9
References: 3

Technical University of Denmark
DTU Wind Energy
Risø Campus
Frederiksborgvej 399
DK-4000 Roskilde

www.vindenergi.dtu.dk

Contents

List of Figures

Chapter 1

Introduction

The long-range WindScanner system is a multi-lidar instrument (Figure 1.1). It consists of three spatially separated pulsed coherent Doppler scanning lidars (for simplicity named WindScanners) and a master computer [1]. Each WindScanner is capable of performing arbitrary scanning trajectories and each has control over its laser pulse emission and steering, and acquisition and analysis of the backscattered light. Thus each WindScanner controls the entire measurement process. The role that the master computer has in the system is to coordinate the ensemble by preparing the WindScanners to perform measurement scenarios; issuing the start time of the measurements, monitoring WindScanners's activities (i.e. measurement process), and intervening if necessary (e.g. synchronizing WindScanners).

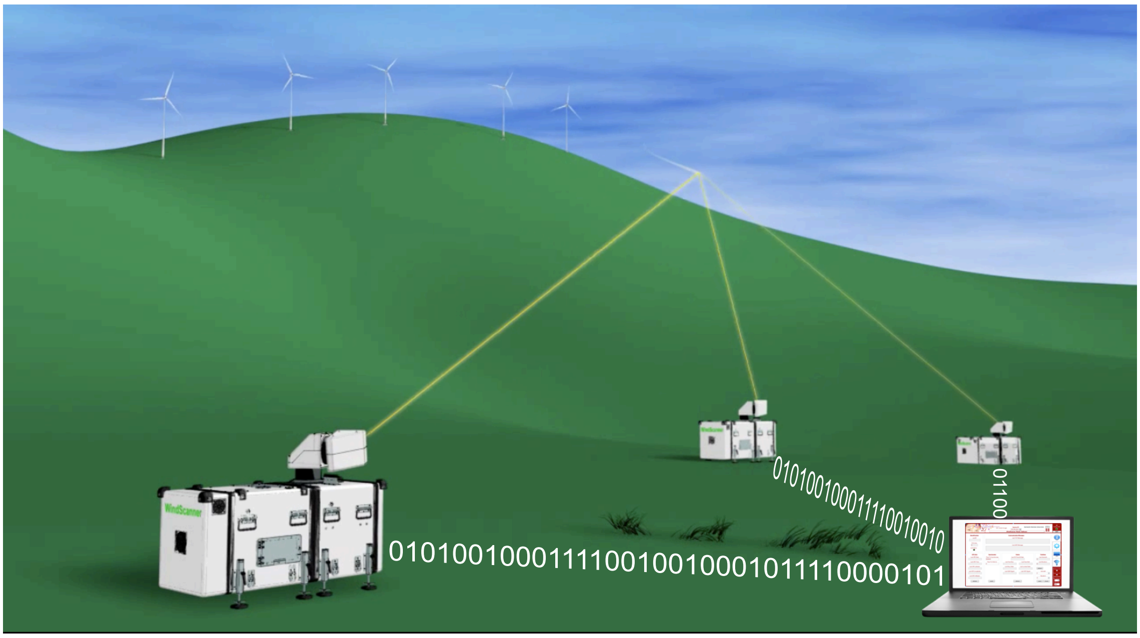


Figure 1.1: Long-range WindScanner system

The coordination of the WindScanners is achieved by the exchange of network packets between the master computer and the WindScanners through a UDP/IP and TCP/IP network. This communication framework between the master computer and the WindScanners has been defined by the Remote Sensing Communication Protocol (RSComPro)

[2, 3]. The network packets, which encapsulate the commands and responses defined by RSComPro, are typically 600 bytes in size, and thus it is possible to use mobile networks such as 3G to achieve the coordination of the WindScanners by the master computer.

The guidelines of RSComPro suggest that the master computer and WindScanners should have static IP addresses in the network, which enable their communication. This suggestion was applied for the development of the WindScanner Client Software (WCS) and Master Computer Software (MCS) [1]. Therefore, to run the long-range WindScanner system over a mobile network it is necessary to provide the WindScanners and master computer with static public IP addresses.

However, acquiring a static public IP address for a mobile connection introduces additional fees and contractual obligations (e.g. contract length) with a mobile operator which can vary from one country to another. We envisage frequent short-term experiments (up to a few months) with the long-range WindScanner system in different countries. In order to support this we would need to acquire the static public IP addresses from different mobile operators, which can be bureaucratically laborious and expensive on a long term.

To avoid these issues in this report we present a network architecture based on a Virtual Private Network (VPN) and mobile network connections without static public IP addresses.

Chapter 2

Approach

A VPN provides means to extend a private network across the Internet. Since a VPN forms a virtual point-to-point connection between computers, it enables computers to exchange data as if they were in the same network. With a VPN it is possible to configure private static IP addresses for each entity in the network.

By using a VPN, we are able to achieve a functional long-range WindScanner system in which the WindScanners and the master computer are in different geographical locations and connected to the Internet with different network connections.

There are different VPN solutions on the market. In the case of the long-range WindScanner system we have selected the hardware solution based on the dedicated network appliances Z1 and MX60 from Cisco Meraki.

2.1 Network appliances

The Z1 has been particularly designed for a teleworker that needs an easy and secure access to company servers while working in a remote location. This appliance is a firewall and VPN gateway with four Gigabit Ethernet ports for the connection of devices (i.e. computers), one Gigabit Ethernet WAN port, one USB port for the connection of a 3G or 4G dongle and a dual-radio 802.11n wireless connection (Figure 2.1).

The MX60 has more processing power and it is suitable for the connection of up to 50 clients. It is a small branch security appliance combined with a VPN gateway. The MX60 has similar connectivity as the Z1, apart from lack of the 802.11n wireless connection. Both appliances are managed using a cloud-based framework.

From the above mentioned characteristics, we can see that the Z1s are suitable for the connection of individual WindScanners to the VPN network. Since the MX60 can handle more incoming connections from clients, it is suitable for the connection of the master computer to the VPN network.

2.2 Network architecture and setup

The proposed network architecture of the long-range WindScanner system using the Cisco Meraki appliances is depicted in Figure 2.3. Each WindScanner comes with two Ethernet

Figure 2.1: Z1 front and back panel

Figure 2.2: MX60 front and back panel

cards. One of them is used to connect a WindScanner to a Z1. The necessary internet connection for the Z1 is provided by connecting a USB dongle with an appropriate SIM card. For clarity in Figure 2.3 the dongles allow 3G connections. Similarly, we connect the master computer Ethernet card via RJ45 to the MX60, and provide the network interface using a USB dongle equipped with a SIM card. Typically the master computer is a laptop PC, which runs the MCS.

Using Meraki Dashboard , a cloud-based framework, we configure the subnet and IP address for each Meraki appliance. Also, using the framework we setup the VPN. Depending on the subnet of the network appliances we configure the static private IP addresses of the Ethernet cards of the WindScanners and the master computer. By doing this we allow a virtual point-to-point connection among the WindScanners and master computer, which in our case, means that the MCS and WCS can exchange network packets.

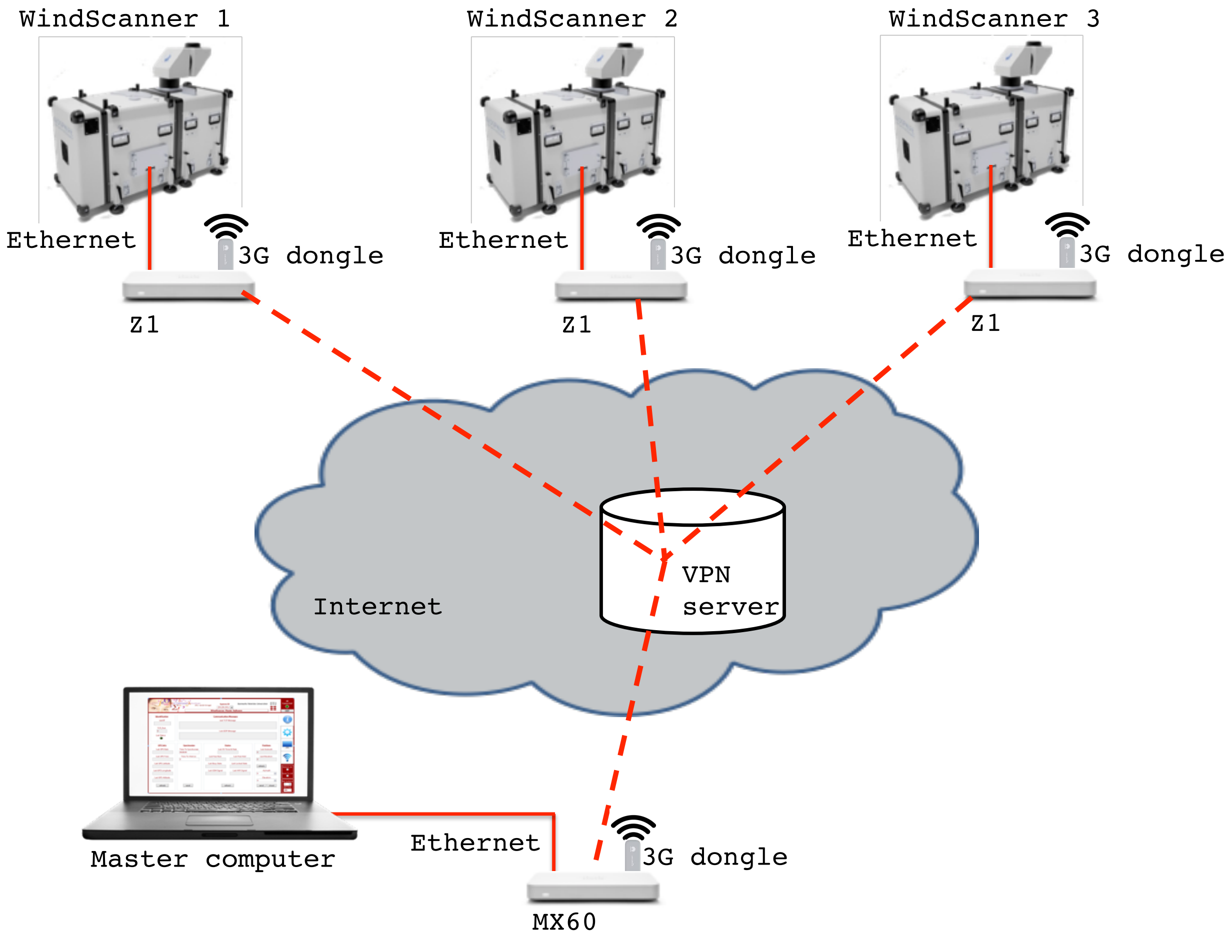


Figure 2.3: Network architecture

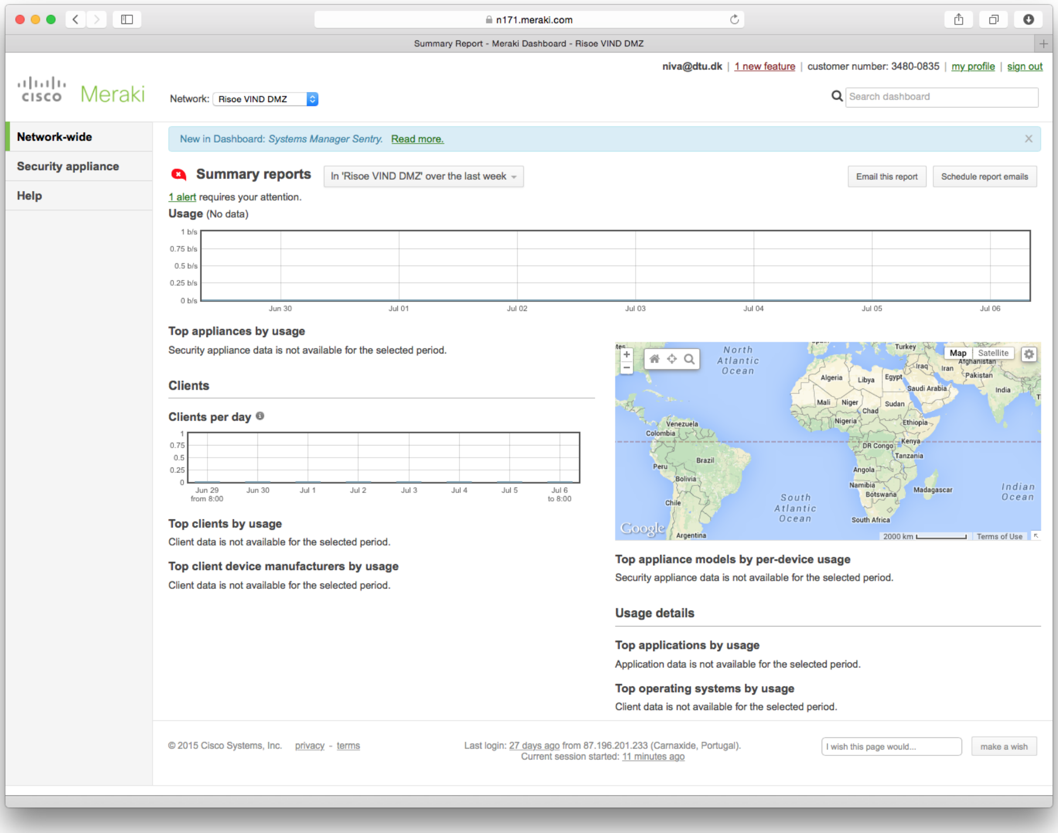


Figure 2.4: Meraki Dashboard

Chapter 3

Conclusion

In this report we have presented the network architecture of the long-range WindScanner system that allows utilization of mobile network connections without the use of static public IP addresses. The architecture mitigates the issues of additional fees and contractual obligations that are linked to the acquisition of the mobile network connections with static public IP addresses. The architecture consists of a hardware VPN solution based on the network appliances Z1 and MX60 from Cisco Meraki with additional 3G or 4G dongles. With the presented network architecture and appropriate configuration, we fulfill the requirements of running the long-range WindScanner system using a mobile network such as 3G. This architecture allows us to have the WindScanners and the master computer in different geographical locations, and in general facilitates deployments of the long-range WindScanner system.

Bibliography

[1] Nikola Vasiljevic. *A time-space synchronization of coherent Doppler scanning lidars for 3D measurements of wind fields*. PhD thesis, 2014. [Cited on pages 1 and 2.]

[2] Nikola Vasiljevic, Guillaume Lea, Michael Courtney, Jörge Schneemann, Davide Trabucchi, Juan-José Trujillo, Robert Unguran, and Juan-Pablo Villa. *The application layer protocol: Remote Sensing Communication Protocol (RSComPro)*. DTU Wind Energy E 0017 (EN). DTU Wind Energy, 2013. [Cited on page 2.]

[3] Nikola Vasiljevic and Juan-José Trujillo. Rscompro: An open communication protocol for remote sensing systems. In *17th International Symposium for the Advancement of Boundary-Layer Remote Sensing*, February 2014. [Cited on page 2.]